



Department Source: City Utilities - Water and Light

To: City Council

From: City Manager & Staff

Council Meeting Date: February 21, 2022

Re: Authorizing a Cyber Security Supply Chain Risk Management Agreement between Open Systems International, Inc. and the City of Columbia

Executive Summary

Staff has prepared for Council consideration an ordinance authorizing the City Manager to execute a Cyber Security Supply Chain Risk Management Agreement with Open Systems International, Inc., the provider of the City's electric Energy Management System. This agreement will ensure that City is in compliance with NERC Standard CIP-013-1 R1 which requires a documented supply chain cyber security risk management plan.

Discussion

Columbia Water and Light, as a Registered Entity with the National Electric Reliability Corporation (NERC) and our designated regional entity, SERC Reliability Corporation, is required to develop one or more documented Supply Chain Cyber Security Risk Management and related implementation plans for its "Medium Impact" Bulk Electric System (BES) cyber systems due to the issuance of a new CIP-013-1 "Cyber Security-Supply Chain Risk Management" as of July 1, 2020.

Compliance Enforcement Authorities (CEAs), namely, National Electric Reliability Corporation (NERC) and our designated Regional Entity - SERC Reliability Corporation, under Section 215 of the Federal Power Act, are required to monitor compliance with the NERC Critical Infrastructure Protection (CIP) Reliability Standards. CIP-013-1 Cyber Security – "Supply Chain Risk Management" went into full effect on July 1, 2020. The purpose of this NERC CIP standard is to mitigate cyber security risks to the reliable operation of the BES by implementing security controls for supply chain risk management of BES Cyber Systems.

The Columbia Water and Light Department (CWLD), as a Registered Entity with NERC, is required to demonstrate and provide evidence to NERC/SERC the City's ability to meet and/or exceed the requirements and sub-requirements of the CIP-013-1 Reliability Standard as it applies to the CWLD's "Medium Risk classification" for Cyber Systems.

CIP-013-1 requirement R1 directs Responsible Entities to "develop one or more documented supply chain cyber security risk management plan(s)" that include processes to use in BES Cyber System procurement that will require vendor cooperation to protect the security of the BES Cyber System supply chain. Responsible Entities will address these requirements by, among other means, inserting contract terms that address the R1.2 security control requirements in agreements with vendors.



City of Columbia

701 East Broadway, Columbia, Missouri 65201

This agreement satisfies the CIP-013-1 requirement R1 by providing a cyber-security risk management plan with Open Systems International, Inc. (OSI). OSI is the provider of the City's electric Energy Management System which provides supervisory control and situational awareness of the Bulk Electric System under the management of the Columbia Water and Light Department.

Fiscal Impact

Short-Term Impact: There are no fiscal impacts due to this agreement. Funds are budgeted each year in the operating budget to pay OSI, Inc. for maintenance and support of the Energy Management System

Long-Term Impact: There are no fiscal impacts due to this agreement. Funds are budgeted each year in the operating budget to pay OSI, Inc. for maintenance and support of the Energy Management System

Strategic & Comprehensive Plan Impact

Strategic Plan Impacts:

Primary Impact: Reliable Infrastructure, Secondary Impact: Not Applicable, Tertiary Impact: Not Applicable

Comprehensive Plan Impacts:

Primary Impact: Infrastructure, Secondary Impact: Not applicable, Tertiary Impact: Not Applicable

Legislative History

Date	Action
06/01/2015	R95-15 Open Systems International Software License Agreement

Suggested Council Action

Approval of the ordinance.